Network Security Assessment Report

Educational Security Analysis

Report Date: December 07, 2025

Total Targets: 1

Total Scans: 10

Assessment Type: Network Reconnaissance & Port Analysis

DISCLAIMER: This report was generated for educational purposes only as part of an Introduction to Security course. All scanning activities were conducted with proper authorization and in accordance with applicable laws and policies.

Executive Summary

This report presents the findings of a network security assessment conducted on 1 target(s). The assessment utilized various reconnaissance techniques covered in the Introduction to Security curriculum to identify active hosts, open ports, and running services.

Assessment Statistics

Metric	Count
Total Scans Performed	10
Successful Scans	8
Failed Scans	2
Hosts Up	8
Hosts Down	0
Total Open Ports Found	12
Unique Services Detected	2

Services Identified

http, ssh

Assessment Methodology

This assessment employed multiple reconnaissance techniques to gather information about the target network. All techniques used are standard practices in the field of information security and are covered in introductory security courses. Below is a description of each technique and its purpose in security assessments.

Host Discovery (Ping Scan)

Command: `nmap -sn [target]`

Purpose: Identifies which hosts are active on the network without performing port scanning. This is the first step in network reconnaissance, helping to map the attack surface.

> ***Security Relevance:*** *An attacker uses this to identify potential targets before launching more aggressive scans. Essential for efficient reconnaissance.*

TCP Connect Scan

Command: `nmap -sT [target]`

Purpose: Establishes full TCP connections to determine which ports are open. This is the most basic form of port scanning and does not require elevated privileges.

> ***Security Relevance:*** *While more detectable, this scan provides reliable information about accessible services. Defenders can easily detect and log these connection attempts.*

TCP SYN Scan (Stealth Scan)

Command: `nmap -sS [target]`

Purpose: Sends TCP SYN packets without completing the three-way handshake, making it less likely to be logged by the target system.

> ***Security Relevance:*** *Considered "stealthy" because it doesn't establish full connections. Commonly used by both security professionals and attackers for reconnaissance.*

Service Version Detection

Command: `nmap -sV [target]`

Purpose: Probes open ports to determine the exact service and version information, which is critical for vulnerability assessment.

> ***Security Relevance:*** *Enables identification of outdated or vulnerable software versions. This is a key step in the vulnerability assessment process.*

Top Ports Scan

Command: `nmap --top-ports 20 [target]`

Purpose: Quickly scans the most commonly used ports, providing rapid results for initial assessment.

> ***Security Relevance:*** *Efficient for quick reconnaissance when time or resources are limited. Focuses on ports most likely to be exploitable.*

Detailed Findings

Target: scanme.nmap.org

Host Status: UP

Scans Performed:

• Host Discovery (Ping Scan) at 2025-12-07T00:04:04.014637
Security Purpose: Reconnaissance - First step to map active hosts before deeper scanning

• TCP Connect Scan at 2025-12-07T00:04:05.517825
Security Purpose: Reconnaissance - Identifies open TCP ports by completing the 3-way handshake

• TCP SYN Scan (Stealth) at 2025-12-07T00:04:11.689983
Security Purpose: Reconnaissance - Stealthier port detection, less likely to be logged

• Service Version Detection at 2025-12-07T00:04:18.738065
Security Purpose: Enumeration - Identifies specific software versions for vulnerability assessment

• Top Ports Scan at 2025-12-07T00:04:36.108541
Security Purpose: Reconnaissance - Quick scan of most likely vulnerable services

• Host Discovery (Ping Scan) at 2025-12-07T00:04:37.141334
Security Purpose: Reconnaissance - First step to map active hosts before deeper scanning

• TCP Connect Scan at 2025-12-07T00:04:38.571523
Security Purpose: Reconnaissance - Identifies open TCP ports by completing the 3-way handshake

• TCP SYN Scan (Stealth) at 2025-12-07T00:04:44.363737
Security Purpose: Reconnaissance - Stealthier port detection, less likely to be logged

• Service Version Detection at 2025-12-07T00:04:49.755443
Security Purpose: Enumeration - Identifies specific software versions for vulnerability assessment

• Top Ports Scan at 2025-12-07T00:05:15.474356
Security Purpose: Reconnaissance - Quick scan of most likely vulnerable services

Open Ports Discovered:

Port	Protocol	Service	Version/Details
22	tcp	ssh	-
80	tcp	http	-
22	tcp	ssh	-
80	tcp	http	-
22	tcp	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80	tcp	http	Apache httpd 2.4.7 ((Ubuntu))
22	tcp	ssh	-
80	tcp	http	-
22	tcp	ssh	-

80	tcp	http	-
22	tcp	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80	tcp	http	Apache httpd 2.4.7 ((Ubuntu))

Security Implications:
This target has 12 open port(s), indicating active services that could potentially be exploited if vulnerabilities exist. Each open port represents a potential attack vector and should be evaluated for security hardening.

Conclusions and Learning Outcomes

Summary of Findings

This assessment successfully identified 8 active host(s) and discovered 12 open port(s) across all targets. A total of 2 unique service type(s) were identified, including: http, ssh. These findings demonstrate the effectiveness of systematic network reconnaissance in identifying potential security exposures.

Educational Takeaways

• **Reconnaissance is Critical:** Understanding the network landscape is the first step in both offensive and defensive security operations.

• **Layered Approach:** Different scan types provide different types of information. Host discovery, port scanning, and service detection work together to build a complete picture.

• **Stealth vs. Accuracy:** Different scan techniques offer trade-offs between stealth and accuracy. SYN scans are stealthier but require elevated privileges.

• **Service Enumeration:** Identifying specific software versions is crucial for vulnerability assessment and exploit development.

• **Legal and Ethical Considerations:** Network scanning should only be performed with explicit authorization. Unauthorized scanning is illegal in most jurisdictions.

• **Defense Perspective:** Understanding these reconnaissance techniques helps defenders implement better detection and prevention mechanisms.

Security Recommendations

• Minimize exposed services and close unnecessary ports

• Implement network segmentation to limit reconnaissance scope

• Deploy intrusion detection systems (IDS) to detect scanning activities

• Regularly update and patch all network services

• Use firewalls to filter unauthorized connection attempts

• Conduct regular security assessments to identify exposures before attackers do